METODE *VULNERABILITY ASSESSMENT* DALAM PENGUJIAN CELAH KEAMANAN APLIKASI WEB *E-GOVERMENT*

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar
Serjana Komputer pada Program Studi Sistem Informasi
Fakultas Teknik dan Informatika

Oleh :

Nama : Muhammad Arya Ristianto

NIM : 21510006

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS GAJAYANA
MALANG

2025

HALAMAN PENGESAHAN

Judul	:	Metode *Vulnerability Assessment* Dalam Pengujian Celah Keamanan Aplikasi Web *E-Goverment*
Disusun oleh		
Nama	:	Muhammad Arya Ristianto
NIM	:	21510006
Program Studi	:	Sistem Informasi
Fakultas	:	Teknik dan Informatika

Disetujui oleh:

Pembimbing

Fachrudin Pakaja, S.Kom.,M.T.
Tanggal :

Mengetahui,

Dekan Fakultas Teknik dan Informatika	Ketua Program Studi Sistem Informasi
Ir. S. B. P. Handhajani, M.T.	Resti Rahayu, S.Kom., M.M.
Tanggal :	Tanggal :

SKRIPSI

Metode *Vulnerability Assessment* Dalam Pengujian Celah Keamanan Aplikasi Web *E-Government*

Oleh:

Muhammad Arya Ristianto

NIM : 21510006

Telah dipertahankan di depan tim penguji

Tanggal 21 Februari 2025

Tim Penguji,

Penguji 1,	Penguji 2,
Ir. S. B. P. Handhajani, M.T.	I Nyoman Suspita S.T., M.M.

ABSTRAK

Keamanan aplikasi web menjadi aspek krusial dalam era digital saat ini, terutama bagi sistem E-Government yang menyimpan data sensitif masyarakat. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis kerentanan pada website Dinas Pendidikan dan Kebudayaan Kota Malang dengan menggunakan metode *Vulnerability Assessment.* Pengujian dilakukan melalui tahapan *Identification Scope, Information Gathering, Vulnerability Scanning, Exploitation, dan Generating Report*, menggunakan alat seperti OWASP ZAP, Zenmap, dan *Whois lookup*.Hasil penelitian menunjukkan bahwa website yang diuji memiliki 11 kerentanan, dengan 2 risiko menengah, 3 risiko rendah, dan 6 informasi perbaikan.Meskipun website tergolong aman dari ancaman kritis, masih diperlukan perbaikan dalam konfigurasi keamanan untuk mencegah eksploitasi lebih lanjut. Penelitian ini memberikan rekomendasi perbaikan yang dapat diterapkan untuk meningkatkan keamanan aplikasi web *E-Government* dan mengurangi potensi serangan siber.

Kata kunci: Keamanan *Website*, *Vulnerability Assessment, Penetration Testing*, OWASP ZAP.

ABSTRACT

Web application security is a crucial aspect in today's digital era, especially for E-Government systems that store sensitive public data. This research aims to identify and analyze vulnerabilities on the Malang City Education and Culture Office website using the Vulnerability Assessment method. Testing is done through the stages of Identification Scope, Information Gathering, Vulnerability Scanning, Exploitation, and Generating Report, using tools such as OWASP ZAP, Zenmap, and Whois lookup. The results show that the tested website has 11 vulnerabilities, with 2 medium risks, 3 low risks, and 6 repair information. Although the website is classified as safe from critical threats, improvements are still needed in the security configuration to prevent further exploitation. This research provides recommendations for fixes that can be implemented to improve the security of E-Government web applications and reduce the potential for cyber attacks.

Keywords: Website Security, Vulnerability Assessment, Penetration Testing, OWASP ZAP

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa yang telah melimpahkan berkat dan rahmat, sehingga penulis dapat menyelesaikan skripsi dengan judul "Metode *Vulnerability Assessment* Dalam Pengujian Celah Keamanan Aplikasi Web *E-Goverment.*".

Dalam menyelesaikan penulisan skripsi ini penulis telah mendapat banyak bantuan, bimbingan dan semangat dari berbagai pihak. Oleh karena itu, penulis ingin menyampaikan terima kasih kepada:

1. Ibu Ir. S. B. P. Handhajani, M.T selaku Dekan Fakultas Teknik dan Informatika Universitas Gajayana Malang yang selalu memberikan dukungan dan saran-saran yang membangun kepada para mahasiswanya.
2. Ibu Resti Rahayu S.Kom.,M.M., selaku Ketua Program Studi Sistem Informasi Fakultas Teknik dan Informatika
3. Bapak Fachrudin Pakaja, S.Kom.,M.T. selaku dosen pembimbing penyusunan skripsi yang telah bersedia meluangkan waktunya, sehingga penulis dapat menyelesaikan skripsi ini dengan baik.

Penulis berharap semoga skripsi ini dapat membantu dan bermanfaat untuk pembaca.

Malang, Maret 2025

Muhammad Arya Ristianto

DAFTAR ISI

HALAMAN PENGESAHAN ..... **ii**
ABSTRAK ..... **iv**
KATA PENGANTAR ..... **v**
DAFTAR ISI ..... **vii**
DAFTAR GAMBAR ..... **x**
DAFTAR TABEL ..... **xi**
DAFTAR LAMPIRAN ..... **xii**

BAB I PENDAHULUAN **1**
1.1 Latar Belakang 1
1.2 Rumusan Masalah 4
1.3 Tujuan Penelitian 4
1.4 Batasan Masalah 4
1.5 Sistematika Pembahasan 5

BAB II KAJIAN PUSTAKA **6**
2.2 Penelitian Terdahulu 6
2.2 Kajian Teori 9
2.2.1 Penetration Testing 9
2.2.2 Website 12
2.2.3 Pengertian Pengujian 13
2.2.4 Peralatan *Penetration Testing* 14
2.2.5 Penilaian Kerentanan 16
2.3 Kerangka Konsep Penelitian 18

BAB III METODE PENELITIAN **20**
3.3 Jenis Penelitian 20
3.2 Lokasi Penelitian 21
3.3 Populasi dan Sampel 21
3.3.1 Populasi Penelitian 21
3.3.2 Sampel Penelitian 22
3.4 Metode Pengumpulan Data 22
3.4.1 Observasi 23
3.4.2 Wawancara 23
3.4.3 Eksperimen Lab Komputer 23
3.5 Tahapan Penelitian 23

3.6 Pengujian Sistem 25
3.7 Alat Penelitian 25
3.7.1 Whois. 25
3.7.2 Zenmap 25
3.7.3 OWASP ZAP 25

BAB IV HASIL DAN PEMBAHASAN 26
4.1 Deskripsi Umum Penelitian 26
4.2 Peralatan *Software* dan *Hardware* 26
4.2.1 Perangkat *Software* 26
4.2.2 Perangkat *Hardware* 27
4.3 Tahapan Analisis Penelitian 27
4.3.1 *Identification Scope* 27
4.3.2 *Information Gathering* 27
4.3.3 *Vulnerabillity Scanning* 30
4.3.4 *Exploitation* 32
4.3.5 *Generating Report* 32
4.4 Pengujian Sistem 34
4.5 Pembahasan 35
4.5.1 *Content Security Policy (CSP) Header Not Set* 35
4.5.2 *Cross-Domain Misconfiguration* 35
4.5.3 *Cookie with Same-Site Attribute None* 35
4.5.4 *Strict-Transport-Security Header Not Set* 36
4.5.5 *Timestamp Disclosure – Unix* 36
4.5.6 *Session Management Response Identified* 36
4.5.7 *Loosely Scoped Cookie* 37
4.5.8 *Information Disclosure – Suspicious Comment* 37
4.5.9 *Retrieved from Cache Informational* 38
4.5.10 *Re-examine Cache-control Directives* 38
4.5.11 *User Agent Fuzzer* 38

BAB V KESIMPULAN DAN SARAN 39
5.1 Kesimpulan 39
5.2 Saran 39

DAFTAR PUSTAKA 40
LAMPIRAN 43

DAFTAR GAMBAR

Nomor	Gambar	Halaman
1. 1	Arsip Serangan Terhadap Dikbud Malang.....	2
2. 1	Kerangka Berfikir *Vulnerability Assessment*	21
3. 1	Tahapan Penelitian.....	26
4. 1	Hasil Pengecekan Whois.....	31
4. 2	Hasil *Scan* Zenmap	32
4. 3	Proses *Scan* OWASP ZAP	33
4. 4	Hasil *Scan* OWASP ZAP	33
4. 5	Hasil Penetrasi OWASP ZAP	34

DAFTAR TABEL

Nomor	Tabel	Halaman
2. 1	Hasil Penelitian oleh Candra Darmawan, dkk. (2024).....	9
2. 2	Penelitian Terdahulu	10
4. 1	Hasil Scanning Zenmap	32
4. 2	Daftar Kerentanan	34
4. 3	Hasil Scanning Whois	35
4. 4	Hasil Scanning Zenmap	35
4. 5	Daftar Kerentanan	36

DAFTAR LAMPIRAN

Nomor	Lampiran	Halaman
1	Surat Pengantar dan Surat Izin……	48
2	Laporan Hasil Uji Menggunakan OWASP ZAP..	50

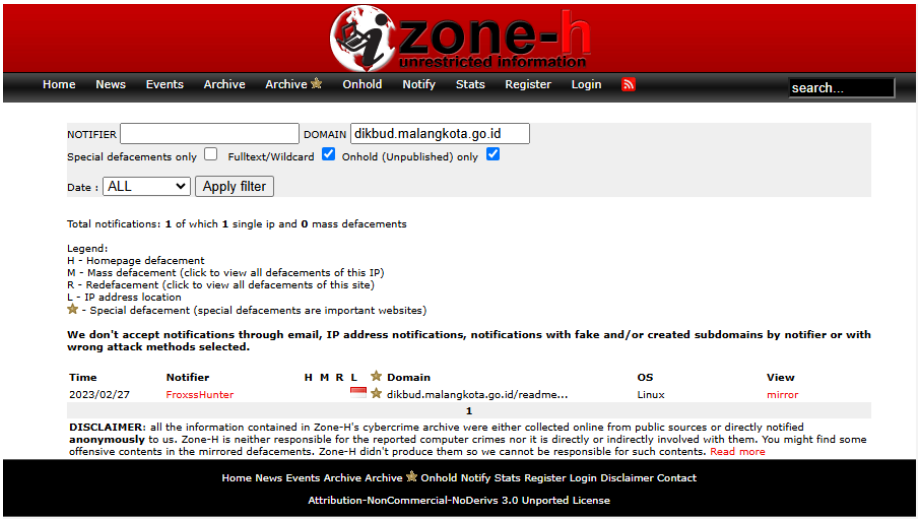
BAB I
PENDAHULUAN

1.1 Latar Belakang

Bocornya data dan informasi serta pencurian kekayaan intelektual merupakan masalah terbesar dalam tindakan *cybercrime* (Riskiyadi & Anggono 2021). Di dalam konteks dunia yang saat ini saling terhubung dan bergantung pada sektor teknologi informasi, keamanan informasi menjadi sangat penting. Apalagi dewasa ini sistem informasi bukan lagi hanya menjadi pendukung bagi sebuah organisasi untuk menunjang proses bisnisnya, akan tetapi menjadi bagian penting dalam menunjang keberhasilan sebuah organisasi hingga menentukan keputusan penting didalamnya. Sehingga keamanan data dan informasi yang terkandung di dalam sistem informasi menjadi suatu hal yang mutlak untuk dijaga (Farismana & Pramadhana, 2022).

Kementerian Komunikasi dan Informatika (Kemenkominfo) sebagai pengelola PDN menyatakan bahwa telah terjadi peretasan pada tanggal 20 Juni 2024. Peretasan PDN tentu saja merupakan masalah besar bagi keamanan data pemerintah negara, pasalnya PDN itu sendiri merupakan sekumpulan Pusat Data yang digunakan bersama oleh Instansi Pusat dan Pemerintah Daerah sehingga saling terhubung. Peretasan PDN terjadi akibat adanya serangan siber oleh *Brain Cipher* dengan menggunakan *ransomware*, yakni perangkat lunak yang bekerja dengan cepat seperti *virus* untuk dapat mengenkripsi sebuah data. Akibatnya, korban tidak dapat mengakses kembali data miliknya karena penyerang akan mengunci akses data tersebut. Serangan siber ransomware terhadap *server* Pusat Data Nasional Sementara (PDNS) berdampak pada 210 instansi pusat maupun

daerah di Indonesia. Akibat gangguan pada PDN ini, proses PPDB tahun ajaran 2024/2025 di beberapa pemerintah kota mengalami perubahan jadwal (Desty Luthfiani, 2024). Dengan mengetahui jenis dan jumlah serangan yang terjadi, maka keamanan sistem informasi perlu menjadi perhatian berbagai pihak. Adapun pihak yang sering terkena serangan siber yaitu pemerintahan, lembaga keuangan, berita, dan jejaring sosial (Kaur dan Kaur, 2019). Histori dari penyerangan tersebut, dapat diketahui dari salah satu situs arsip defacement, yaitu http://zone-h.org Zone-h adalah arsip yang berisi mirror dari sebagian besar situs web yang diretas. Berikut arsip serangan terhadap Dikbud Kota Malang:



Gambar 1.1 Arsip Serangan Terhadap Dikbud Malang

Dari Zone-h dapat diketahui bahwa Dikbud Malang telah terkena serangan siber berbasis web yakni *web defacement*. Serangan diawali pada tanggal 27 Februari 2023 oleh FroxssHunter pada portal https://dikbud.malangkota.go.id/. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis kerentanan pada

aplikasi web *E-Government* melalui metode *Vulnerability Assessment*. Tujuannya adalah untuk memberikan rekomendasi perbaikan yang efektif untuk meningkatkan keamanan sistem informasi dan melindungi data serta informasi sensitif dari ancaman siber. Tujuan ini sejalan dengan penelitian sebelumnya yang menekankan pentingnya *Vulnerability Assessment* dalam mengidentifikasi kerentanan pada aplikasi web (Al-Shboul et al., 2018).

Penelitian ini sangat relevan dengan konteks keamanan informasi di era digital saat ini, di mana serangan siber semakin kompleks dan berbahaya. Kasus peretasan PDN dan serangan web defacement terhadap Dikbud Malang menjadi bukti nyata bahwa keamanan sistem informasi, khususnya aplikasi web *E-Government*, perlu mendapatkan perhatian serius. Penelitian ini akan memberikan kontribusi penting dalam upaya meningkatkan keamanan aplikasi web *E-Government* dan melindungi data serta informasi masyarakat dari ancaman siber. Hal ini sejalan dengan penelitian sebelumnya yang menekankan pentingnya *Vulnerability Assessment* dalam mengidentifikasi kerentanan pada aplikasi web (Al-Shboul et al., 2018).

Dengan memahami tujuan penelitian dan hubungan dengan objek penelitian, peneliti dapat melihat betapa pentingnya penelitian ini dalam konteks keamanan informasi di era digital, maka dari itu peneliti mengambil topik penelitian melakukan *Vulnerability Assessment* dan *Penetration Testing* terhadap aplikasi web https://dikbud.malangkota.go.id/ dengan judul penelitian "Metode *Vulnerability Assessment* Dalam Pengujian Celah Keamanan Aplikasi Web *E-Government"*. guna mengetahui celah-celah apa saja yang dapat ditembus oleh peretas untuk selanjutnya diperbaiki agar supaya serangan peretas dapat dicegah.

1.2 Rumusan Masalah

Berdasarkan latar belakang, maka dapat diperoleh suatu rumusan masalah sebagai berikut:

1. Bagaimana proses *Penetration Testing* pada *website* Dinas Pendidikan dan Kebudayaan Kota Malang (https://dikbud.malangkota.go.id/)
2. Bagaimana proses mencari celah keamanan pada web Dinas Pendidikan dan Kebudayaan Kota Malang (https://dikbud.malangkota.go.id/)
3. Bagaimana proses yang tepat untuk menutupi kelemahan yang ditemukan pada web https://dikbud.malangkota.go.id/

1.3 Tujuan Penelitian

Berdasarkan uraian masalah, maka tujuan pada penelitian ini adalah:

1. Menganalisis celah keamanan serta melakukan pengukuran tingkat kerentanan sistem informasi pada *website* https://dikbud.malangkota.go.id/.
2. Menganalisis hasil *Vulnerability Assessment dan penetration test* (VAPT) yang diolah ke dalam *report* hasil pengujian.
3. Menganalisis solusi yang tepat untuk menutupi kelemahan yang ditemukan pada *website* https://dikbud.malangkota.go.id/.

1.4 Batasan Masalah

Mengingat begitu luasnya ruang lingkup pada penelitian ini, maka diperlukan suatu batasan sebagai berikut:

1. Penelitian ini dilakukan pada sistem operasi Windows 10 Professional.
2. *Penetration Testing* akan menggunakan beberapa *tools* yaitu Zenmap, OWASP ZAP, *Whois* lookup.

3. *Penetration Testing* dilakukan hanya dalam ruang lingkup *website* https://dikbud.malangkota.go.id/

1.5 Sistematika Pembahasan

Sistematika Penlulisan skripsi ini disusun dengan struktur pembahasan sebagai berikut:

BAB I PENDAHULUAN

Bab ini menjelaskan tentang latar belakang masalah, identifikasi masalah perumusan masalah, batasan masalah, tujuan penelitian, metode penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Menguraikan kajian pustakan dan dasar teori yang berkaitan dengan *Penetration Testing*, *Vulnerability Assessment,* penelitian sebelumnya dan kerangka alur pengujian.

BAB III METODE PENELITIAN

Bab ini akan menjelaskan tentang metode pengujian sistem serta menjelaskan mengapa metode dan teknik tersebut dipilih dalam menyelesaikan masalah yang akan diuji.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi tentang proses pengujian dan analisis masalah dari penelitian dan juga pembahasan yang mencakup gambaran umum tentang objek penelitian.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari uraian pembahasan penelitian serta saran dan kritik agar hasil penulisan selanjutnya dapat lebih baik lagi.

BAB II

KAJIAN PUSTAKA

2.1 Penelitian Terdahulu

Penelitian Pertama (Farismana dan Pramadhana 2023) melakukan penelitian menggunakan metode *Vulnerability Assessment*, dimana penelitian ini berfokus pada tahapan *Information Gathering* dan *Vulnerability Scanning* untuk melakukan pengujian kerentanan menggunakan *tools* vulnerability scanner, kemudian melakukan analisis terhadap hasil pengujian terhadap sistem informasi repositori yang karya ilmiah yang diuji. Berikut tahapan vulnerability assesment yang dilakukan dalam penelitian ini.

Hasil *Vulnerability Assessment* terdapat total sebanyak 22 peringatan dimana terdapat 1 risiko dengan *level high*, 7 risiko *medium*, 9 risiko *low*, dan 5 tingkatan informational. Sedangkan dari sisi confidence terdapat 3 *level high*, 14 *level medium*, dan 5 *level low*. Pada tahap vulnerability analysis risiko dengan *level high* bertambah menjadi 2 dengan presentase 9,1 % dari keseluruhan risiko (Farismana, dan Pramadhana 2023).

Penelitian Kedua (Supriadi dkk. 2024) melakukan penelitian dengan menerapkan metode *Vulnerability Assessment* yang berpedoman pada standar *Open Web Application Security Project (OWASP)*. Metode *Vulnerability Assessment*. Tahapan *Vulnerability Assessment* yang dilaksanakan adalah: *Identification Scope*, *Information Gathering*, *Vulnerability Scanning*, Eksploitasi, *Generating Report*.

Hasil dari audit keamanan pada situs web Universitas Teknologi Mataram, ditemukan total 11 kerentanan yang terdiri dari 3 vulnerabilitas yang memiliki risiko menengah, 4 *vulnerabilitas* yang memiliki risiko rendah, serta 4 kerentanan

informatif. Kerentanan berisiko menengah memerlukan perhatian prioritas dalam upaya perbaikan.

Penelitian Ketiga (Candra Darmawan, dkk. 2024) melakukan penelitan dengan metode *Vulnerability Assessment* yang khusus menguji keamanan jaringan atau sistem aplikasi (Budiman et al., 2021). Tujuan metode penelitian ini agar proses identifikasi celah keamanan sampai proses perbaikan mendapatkan hasil yang maksimal dan terstruktur (Hafitzhah et al., 2023).

Hasil temuan celah kerentanan paling banyak adalah A05:2021 yaitu *Security Misconfiguration* serta paling sedikit A01:2021 yaitu Broken Access Control dan A08:2021 yaitu *Software and Data Integrity Failures*. Hasil membuktikan, konfigurasi sistem dan pengaturan keamanan *website* UNIPA masih belum baik. Perlu dilakukan penanganan serius pada titik ini.

Tabel 2.1 Hasil Penelitian oleh (Candra Darmawan, dkk. 2024)

Alerts ID	***Alerts***	***Risk***	**OWASP ID**
A1	*Absence of Anti-CSRF Tokens*	*Medium*	A01:2021
A2	*Content Security Policy* (CSP) *Header Not Set*	*Medium*	A05:2021
A3	*Missing Anti-clickjacking Header*	*Medium*	A05:2021
A4	*Cross-Domain JavaScript Source File Inclusion*	*Low*	A08:2021
A5	*Strict-Transport-Security Header Not Set*	*Low*	A05:2021
A6	*Timestamp Disclosure – Unix*	*Low*	A01:2021
A7	*X-Content-Type-Options Header Missing*	*Low*	A05:2021

Berikut tampilan penelitian terdahulu dalam bentuk Tabel:

Tabel 2.2 Penelitian Terdahulu

No.	Judul, Peneliti, Tahun Terbit	Metode Penelitian	Hasil
1.	*Vulnerability Assessment* Untuk Analisis Tingkat Keamanan Pada Sistem Informasi Repositori Karya Ilmiah Politeknik XYZ (Farismana dan Pramadhana 2023).	*Vulnerability Assessment*	Terdapat total sebanyak 22 peringatan dimana terdapat 1 risiko dengan *level high*, 7 risiko *medium*, 9 risiko *low*, dan 5 tingkatan informational. Sedangkan dari sisi *confidence* terdapat 3 *level high*, 14 *level medium*, dan 5 *level low*.
2.	Implementasi *Vulnerability Assessment* OWASP Pada *Website* Universitas Teknologi Mataram (Dedi Supriadi dkk. 2024).	*Vulnerability Assessment*	Ditemukan total 11 kerentanan yang terdiri dari 3 vulnerabilitas yang memiliki risiko menengah, 4 vulnerabilitas yang memiliki risiko rendah, serta 4 vulnerabilitas informatif.
3.	Penerapan Metode *Vulnerability Assessment* untuk Identifikasi Keamanan *Website* berdasarkan OWASP ID Tahun 2021 (Candra Darmawan, dkk. 2024).	*Vulnerability Assessment*	Celah kerentanan paling banyak adalah yaitu *Security Misconfiguration* serta paling sedikit yaitu *Broken Access Control* dan *Software and Data Integrity Failures.*

Berdasarkan tabel tersebut, posisi atau objek penelitian yang dikaji sebelumnya adalah sistem informasi repositori dan *website* yang masih berfokus pada lingkup institusi pendidikan (*internal*), sedangkan penlitian yang akan diuji

menitikberatkan pada aplikasi web *E-Government* yang memiliki sensitivitas data tinggi.

2.2 Kajian Teori

2.2.1 *Penetration Testing*

.*Penetration Testing website*, atau yang lebih dikenal dengan istilah web pentest, merupakan sebuah proses pengujian keamanan yang bertujuan untuk mengidentifikasi dan menemukan kerentanan yang ada pada sebuah aplikasi web. Tujuan utama dari web pentest adalah untuk mencari titik lemah atau celah keamanan. Namun, bukan untuk merusak *website*, melainkan untuk mencari dan menemukan kelemahan sebelum pelaku kejahatan siber yang sebenarnya menemukannya dan menggunakannya untuk menyerang (Al-Shboul, Abourdaha, & Shah, 2018).

Penetration Testing Execution Standard (PTES) merupakan sebuah standar baru yang di desain bisnis dan penyedia servis keamanan dengan menggunakan Bahasa yang umum dengan cakupan dalam melakukan *Penetration Testing*. PTES dimulai pada awal tahun 2009 dan berawal dari pertemuan antara anggota pendiri disaat membicarakan tentang kepentingan atau kelemahan dalam *Penetration Testing* yang ada sekarang. Fase PTES didesain untuk menjelaskan sebuah *Penetration Testing* dan memastika *client* bahwa sebuah usaha *level* standarisasi akan diperluas pada *Penetration Testing* oleh semua orang yang melakukan tipe *assestment* ini dengan 7 tahap dalam melakukan *Penetration Testing Execution* (Syarif, T. R, 2019):

1. ***Pre-Engagement Interaction***

   Pada tahap ini akan dilakukan pertukaran informasi, rencana dan persiapan untuk pengujian. Sebelum pengujian berlangsung akan dilakukan pertemuan

antara penulis dan pihak yang akan *Penetration Testing*. Melakukan pertemuan untuk meminta konfirmasi ruang lingkup (scope).

2. ***Intelligence Gathering***

   Merupakan sebuah langkah untuk mendapatkan informasi sebanyakbanyaknya yang dapat dimanfaatkan dalam *Vulnerability Assessment* dan fase eksploitasi. Semakin banyak informasi yang didapat dalam fase ini, semakin banyak serangan yang biasa digunakan di masa yang akan datang.

3. ***Threat Modelling***

   Merupakan sebuah prosedur untuk mengoptimalisasi keamanan network dengan mengidentifikasi tujuan-tujuan dan kelemahan-kelemahan, dan menentukan tindakan balasan untuk mencegah, dan mengurangi efek-efek yang berbahaya untuk system. Di dalam konteks ini serangan-serangan yang berpotensi berbahaya seperti Denial of Service (DOS) atau tak sengaja seperti storage device failure.

4. ***Vulnerabillity Testing***

   Merupakan sebuah proses untuk mendapatkan sebuah kelemahan yang ada di system dan aplikasi yang dapat digunakan oleh penyerang. Kelemahan-kelemahan ini biasa berada pada *host* dan kesalahan konfigurasi ataupun desain aplikasi yang tidak aman. Walaupun proses yang digunakan untuk melihat kelemahan tersebut bervariasi dan sangat bergantung pada komponen-komponen yang yang dicoba.

5. ***Exploitation***

   Merupakan sebuah proses dalam *Penetration Testing* yang berfokus dalam menetapkan akses kedalam sebuah sistem dengan melawati pembatasan

keamanan. Jika vulnerability analysis dilakukan dengan benar, fase ini akan terencana dengan baik dan dengan serangan yang tepat.

6. ***Post Exploitation***

   Tujuan dari fase post *Exploitation* ialah untuk menentukan harga dari system dan untuk mempertahankan kontrol dari sistem agar dapat digunakan untuk nanti. Harga dari sebuah system dapat ditentukan dengan melihat sensitifitas data yang disimpan disana dan kegunaan mesin dalam system yang akan digunakan nanti.

7. ***Reporting***

   Merupakan sebuah langkah untuk menuliskan laporan yang mendeskripsikan hasil lengkap pengujian dan presentasi yang sudah dipersiapkan dengan rekomendasi dan penyelesaiannya.

Menurut penelitian (Andhika, 2023), Metode *Vulnerability Assessment* yang berpedoman pada standar *Open Web Application Security Project (OWASP)* unggul dalam mendeteksi dan menganalisis kerentanan aplikasi web, serta memberikan solusi mitigasi yang efisien untuk memperkuat keamanan sistem. Dengan penerapan *Vulnerability Assessment*, penelitian ini berupaya untuk memberikan penilaian menyeluruh terkait tingkat keamanan sistem serta menyusun rekomendasi perbaikan guna meningkatkan ketahanan terhadap ancaman siber.

Tipe *assestment* ini dilakukan dengan 5 tahap pengujian. Berikut tahapan pengujian yang dilaksanakan:

1. ***Identification Scope***

   Pada tahap ini, ruang lingkup pengujian ditentukan dengan batasan yang dilakukan untuk memastikan bahwa pengujian hanya mencakup area yang relevan dengan tujuan evaluasi keamanan situs web.

2. *Information Gathering*

Tahap pengumpulan informasi bertujuan untuk mengidentifikasi teknologi yang digunakan oleh *website*, termasuk *server*, platform, dan layanan pendukung. Alat yang digunakan dalam tahap ini meliputi *Whois* untuk memperoleh informasi *domain*, Zenmap untuk pemetaan jaringan.

3. *Vulnerability Scanning*

Proses pemindaian kerentanan memanfaatkan OWASP ZAP guna mendeteksi kemungkinan adanya celah keamanan pada situs web.

4. Eksploitation

Tahap ini bertujuan untuk memverifikasi apakah celah keamanan yang ditemukan dapat dieksploitasi oleh penyerang, serta untuk mengukur dampak potensial dari kerentanan tersebut.

5. *Generating Report*

Laporan akhir disusun berdasarkan hasil temuan, mencakup tingkat risiko, serta rekomendasi langkah-langkah mitigasi yang diperlukan untuk meningkatkan keamanan *website*.

2.2.2Website

Website adalah bagian tidak terpisahkan dari perkembangan internet, dan saat ini jumlahnya mencapai 1,9 miliar di seluruh dunia. Awalnya, tujuan penggunaan web adalah untuk pribadi saja. Namun, saat ini hampir semua perusahaan memilikinya. Sebut saja, Facebook, Apple, BBC News dan lainnya, *Website* pertama di dunia dibuat oleh Tim Berners-Lee pada akhir 1980-an. Dalam project *World Wide Web* (W3). Situs web tersebut resmi diluncurkan secara online pada 6 Agustus 1991 dengan URL http://info.cern.ch. (Wijayanti, 2022).

Website, atau yang juga dikenal dengan istilah situs web, merupakan kumpulan halaman web yang saling terkait dan dapat diakses melalui jaringan internet. Sebuah *website* biasanya размещается pada sebuah *server* web dan memiliki alamat unik yang disebut dengan nama *domain*. *Website* dapat berisi berbagai jenis informasi, seperti teks, gambar, video, audio, dan bahkan aplikasi interaktif (Ibrahim & Khan, 2016).

2.2.3 Pengertian Pengujian

Pengujian adalah satu set aktifitas yang direncanakan dan sistematis untuk menguji atau mengevaluasi kebenaran yang diinginkan. Aktifitas pengujian terdiri dari satu set atau sekumpulan langkah dimana dapat menempatkan desain kasus uji yang spesifik (Nur Cholifah, 2018:207).

2.2.3.1 *Black-box Testing*

Black-box Testing adalah metode pengujian di mana penguji tidak memiliki pengetahuan tentang struktur internal atau kode sumber dari aplikasi yang diuji. Dalam konteks *Penetration Testing*, *Black-box Testing* mensimulasikan serangan dari perspektif penyerang yang tidak mengetahui detail sistem, yang memungkinkan identifikasi kerentanan yang dapat dieksploitasi dari luar. Penguji hanya berfokus pada input dan output, mengevaluasi apakah *website* berfungsi seperti yang diharapkan tanpa mempertimbangkan bagaimana fungsionalitas tersebut diimplementasikan (Maia & D'Ambrosio, 2020).

2.2.3.2 *White-box Testing*

White-box Testing, di sisi lain, adalah metode di mana penguji memiliki akses penuh terhadap kode sumber, struktur internal, dan desain aplikasi yang diuji. Dalam konteks *Penetration Testing*, ini memungkinkan penguji untuk melakukan

analisis mendalam mengenai potensi kerentanan dalam kode, serta memahami alur logika dan jalur eksekusi yang mungkin tidak terlihat dalam pengujian black-box. Pendekatan ini bertujuan untuk mengidentifikasi dan memperbaiki kerentanan yang ada sebelum aplikasi dirilis, serta memastikan bahwa semua aspek sistem telah diperiksa secara menyeluruh (Leszczyna, 2021).

2.2.3.3 *Grey-box Testing*

Grey-box Testing merupakan kombinasi dari black-box dan white-box testing, di mana penguji memiliki pengetahuan terbatas tentang kode sumber dan arsitektur sistem yang diuji. Dalam konteks *Penetration Testing*, metode ini memungkinkan penguji untuk memanfaatkan pengetahuan yang ada tentang elemen internal untuk merancang uji yang lebih efektif, sekaligus melihat bagaimana aplikasi berfungsi dari perspektif pengguna. Dengan pendekatan ini, penguji dapat lebih fokus pada area tertentu yang berpotensi rentan sambil tetap mempertahankan pendekatan yang tidak sepenuhnya terbatas pada sikap internal (Khan et al., 2019).

2.2.4 Peralatan *Penetration Testing*

Peralatan pentest, atau yang juga dikenal dengan istilah *Penetration Testing tools*, adalah sekumpulan perangkat lunak dan perangkat keras yang digunakan oleh para ahli keamanan siber untuk melakukan pengujian penetrasi (*Penetration Testing*). Pengujian penetrasi sendiri merupakan sebuah proses simulasi serangan siber yang bertujuan untuk mengidentifikasi dan mengeksploitasi kerentanan yang ada pada sebuah sistem atau jaringan (Verma & Sharma, 2017).

Peralatan pentest sangat beragam, mulai dari perangkat lunak sederhana seperti port scanner hingga perangkat lunak yang lebih kompleks seperti framework

pengujian penetrasi. Beberapa contoh peralatan pentest yang umum digunakan antara lain:

2.2.4.1 OWASP ZAP

OWASP adalah sebuah organisasi nirlaba yang fokus pada keamanan web app. OWASP banyak menyediakan sumber daya agar Anda bisa mempelajari lebih lanjut tentang keamanan web app. Sebagai salah satu prinsipnya, OWASP memastikan bahwa semua informasi dan materi pembelajarannya bisa diakses dengan mudah dan gratis sehingga semua orang bisa meningkatkan keamanan *website* mereka. Materi yang mereka sediakan berupa dokumentasi, *tools*, video, dan forum. Zed Attack Proxy (ZAP) adalah aplikasi untuk melakukan pentest untuk menemukan vulnerabilities dalam suatu web applications dengan cara mudah, ZAP menyediakan scanner automatis sebaik bila kita menggunakan tool untuk menemukan vulnerabilities secara manual. Ketika digunakan sebagai *server*proxy, ini memungkinkan pengguna untuk memanipulasi semua lalu lintas yang melewatinya, termasuk lalu lintas menggunakan https, itu juga dapat berjalan dalam mode daemon yang kemudian dikontrol melalui REST API. ZAP telah ditambahkan ke dalam Radar Teknologi ThoughtWorks pada 30 Mei 2015 di cincin Percobaan. ZAP awalnya bercabang dari Paros, proxy pentesting lainnya. Simon Bennetts, pemimpin proyek, menyatakan pada tahun 2014 bahwa hanya 20% dari kode sumber ZAP masih dari Paros (Riyan Farismana, dkk. 2023).

2.2.4.2 *Whois*

Secara garis besar, *Whois* adalah sebuah layanan di internet yang berfungsi untuk mengetahui data atau informasi tentang suatu *domain* tertentu. Layanan ini menyediakan dan menampilkan informasi kepemilikan *domain*, misalnya nama

pemilik, kontak, alamat, dan sebagainya. Dengan kata lain, *Whois* bisa dianalogikan sebagai address book besar berisi kumpulan data *domain* yang bisa dilihat oleh siapapun (Nurul Huda, 2022).

2.2.4.3 Zenmap

Perangkat lunak Zenmap merupakan aplikasi *multi platform* sebagai interface sederhana untuk apikasi nmap. Nmap *(Network Mapper)* sendiri adalah sebuah aplikasi *open-source* untuk explorasi network dan audit keamanannya (Nur Cholifah, 2018). Zenmap memiliki beberapa pilihan profil untuk melakukan *Scanning* berikut ini adalah profil yang sering digunakan dalam zenmap:

a) *Intense scan*

Intense scan merupakan profil dimana perintah scan meliputi *port-port* yang terbuka, model topologi jaringan dari target yang di *scan*, *service* yang sedang aktif, serta *host detail* yang berisikan informasi sistem operasi target dan persentase ketepatan hasil scan.

b) *Intense scan plus UDP*

Profil ini hampir sama dengan intense scan, namun ditambah dengan port-port UDP yang sedang aktif.

c) *Intense scan, all TCP ports*

Profil ini juga sama dengan *intense scan* dan ditambah melakukan *Scanning* nomor *port* dimulai dari nomor 1 hingga nomor *port* 65535.

2.2.5 Penilaian Kerentanan

Penilaian kerentatan keamanan (*Vulnerability Assessment*) adalah proses utama perbaikan menuju kepada kematangan dan intergrasi sistem keamanan informasi. Sedangkan Pengujian Penetrasi *(Penetration Testing*) hanya potret

efektifitas sistem keamanan informasi yang sudah diterapkan saat potret dilakukan. Karena dasar inilah, tanpa bermaksud mengesampingkan Pengujian Penetrasi, Penilaian Kerentanan dapat memberikan nilai tambah lebih kepada organisasi dibandingkan dengan Pengujian Penetrasi atas pentingnya Sistem Manajemen yang efisien (Itg.id, 2021).

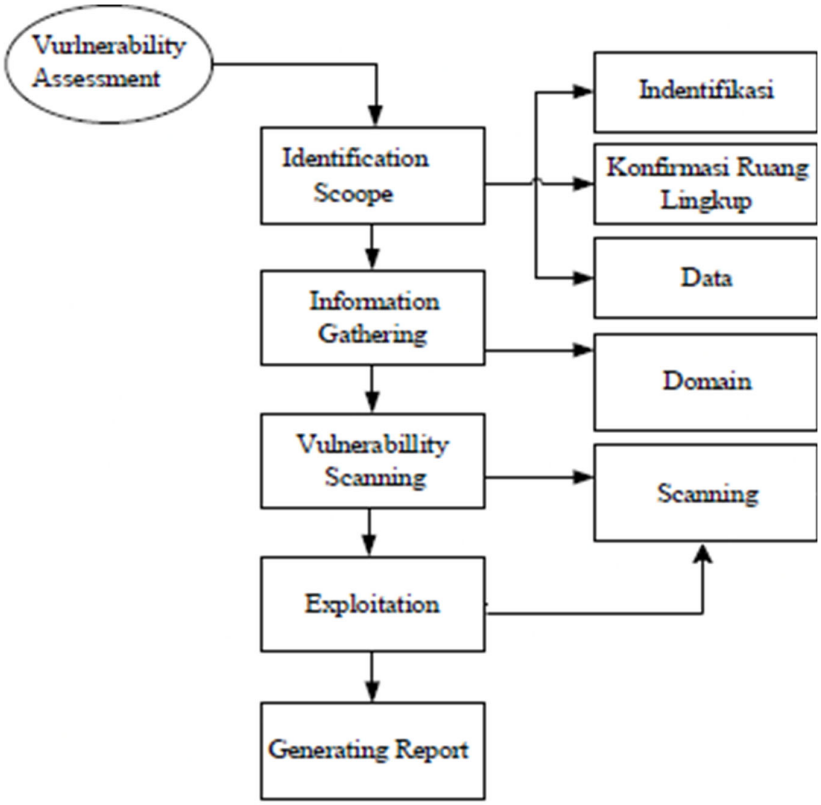
Sepuluh risiko keamanan telah diidentifikasi oleh *Open Web Application Security Project (OWASP)* sebagai risiko keamanan paling kritis yang terkait dengan aplikasi web. Risiko ini dikenal sebagai bentuk serangan yang umum. Selain dapat dieksploitasi dan dapat berdampak negatif pada situs web saat dijalankan, maka mereka dimasukan sebagai peringkat 10 besar risiko teratas yang dipublikasikan oleh OWASP yaitu, (Appiah et al., 2019):

a) *Injection flaws*
b) *Broken authentication and session management*
c) *Cross site scripting*
d) *Insecure direct object references*
e) *Security misconfiguration*
f) *Sensitive data exposure*
g) *Missing level access control*
h) *Cross Site Request Forgery (CSRF)*
i) *Using components with known vulnerabilities*
j) *Unvalidated redirects and forwards*

Melalui identifikasi kerentanan keamanan web dari hasil reporting, akan diberikan saran/solusi guna meningkatkan tingkat keamanan *website* aplikasi sampai mencapai *level* rendah (*low*).

2.3 Kerangka Konsep Penelitian

Dalam rencana pengujian kerangka berfikir *Penetration Testing* yang akan diuji yaitu terlihat pada Gambar 2.1:



Gambar 2.3 Kerangka Berfikir *Vulnerability Assessment*

Proses pada kerangka pengujian tersebut dimulai dengan identifikasi ruang lingkup, yaitu menentukan apa saja yang akan diuji, meminta izin dan memastikan batasan atau area yang perlu dianalisis. Selanjutnya, dilakukan pengumpulan informasi (*information gathering*) untuk mendapatkan data serta domain yang relevan. Setelah data terkumpul, proses berlanjut ke pemindaian kerentanan (*vulnerability scanning*) guna mendeteksi kemungkinan celah keamanan. Jika

ditemukan kerentanan, tahap eksploitasi dilakukan untuk menguji sejauh mana celah tersebut dapat dimanfaatkan. Terakhir, seluruh temuan dan hasil pengujian didokumentasikan dalam laporan (generating report), sehingga dapat ditindaklanjuti untuk perbaikan keamanan.

BAB III

METODE PENELITIAN

3.1 Jenis Penelitian

Studi kasus eksperimen merupakan jenis penelitian yang menggabungkan pendekatan studi kasus dengan desain eksperimental, di mana peneliti tidak hanya mendalami konteks alami dari suatu fenomena, tetapi juga menerapkan intervensi terkontrol untuk menguji hubungan sebab-akibat antar variabel. Dengan mengintegrasikan metode kualitatif dan kuantitatif, pendekatan ini memungkinkan pengumpulan data yang komprehensif serta pengujian hipotesis melalui manipulasi variabel secara sistematis. Metode ini memberikan validitas internal yang kuat melalui kontrol eksperimental dan validitas eksternal yang tinggi karena dilaksanakan dalam setting nyata, sehingga hasil penelitian dapat langsung diaplikasikan dalam konteks dunia riil (Johnston & Becker, 2020).

Dalam implementasinya, studi kasus eksperimen menuntut perencanaan yang cermat mulai dari penentuan ruang lingkup penelitian, pengumpulan data kontekstual, penerapan intervensi, hingga evaluasi dampak dari perlakuan yang diberikan. Pendekatan ini memungkinkan peneliti mengidentifikasi faktor-faktor kunci yang mempengaruhi hasil serta memahami mekanisme kausal secara mendalam. Penelitian terbaru telah menunjukkan bahwa integrasi antara studi kasus dan desain eksperimen dapat meningkatkan keakuratan analisis serta memberikan rekomendasi yang lebih tepat guna dalam pengambilan keputusan strategis (Martinez, F., & Zhao, L. 2021).

Alasan penulis menggunakan jenis penelitian studi kasus eksperimen karena pendekatan ini memungkinkan penggabungan keunggulan analisis mendalam

secara kontekstual dengan kemampuan untuk menguji hubungan sebab-akibat melalui manipulasi variabel secara terkontrol (desain eksperimen). Dengan demikian, metode ini memberikan validitas internal yang tinggi karena adanya kontrol eksperimental serta validitas eksternal yang baik karena penelitian dilakukan dalam setting nyata (Martinez, F., & Zhao, L. 2021).

3.2 Lokasi Penelitian

Menurut Winarta Sujarweni (2014:73) Lokasi penelitian adalah tempat dimana penelitian itu dilakukan. Oleh karena itu, dapat disimpulkan bahwa lokasi penelitian adalah tempat peneliti melakukan proses studi untuk memperoleh data dan memecahkan masalah dalam penelitian yang sedang dilakukan serta mempermudah peneliti dalam melakukan penelitian kerena telah memiliki objek dan lokasi yang jelas.

Dengan Judul penelitian adalah "Metode *Vulnerability Assessment* Dalam Pengujian Celah Keamanan Aplikasi Web *E-Government",* penulis memilih waktu penelitian dilakukan dari 4 Desember 2024 hingga 4 Januari 2025, dengan lokasi penelitian di Dinas Pendidikan dan Kebudayaan Kota Malang yang beralamat di Jl. Veteran No. 19, Ketawanggede, Kec. *Low*okwaru, Kota Malang, Jawa Timur 65145, Indonesia.

3.3 Populasi dan Sampel

3.3.1 Populasi Penelitian

Populasi yang menjadi fokus peneliti adalah seluruh aplikasi web *E-Government* yang dioperasikan oleh Dinas Pendidikan Kota Malang, khususnya *website* https://dikbud.malangkota.go.id/. Aplikasi ini memiliki sejumlah fitur yang

melayani kebutuhan masyarakat, sehingga penting untuk memastikan bahwa keamanan dan integritas datanya terjaga dengan baik. Dalam konteks ini, peneliti akan melakukan analisis menyeluruh terhadap infrastruktur keamanan *website* tersebut, guna mengidentifikasi potensi kerentanan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab.

3.3.2 Sampel Penelitian

Untuk sampel dalam penelitian ini, peneliti akan fokus pada modul-modul kunci dalam *website* dikbud.malangkota.go.id yang sering digunakan oleh pengguna, termasuk sistem pendaftaran, pengumuman, dan layanan informasi. Pemilihan modul-modul ini didasarkan pada frekuensi aksesnya dan signifikansinya dalam memberikan layanan publik. Dengan demikian, penelitian ini tidak hanya bertujuan untuk mengungkap kerentanan yang ada, tetapi juga untuk memberikan rekomendasi yang bisa diambil untuk meningkatkan keamanan keseluruhan aplikasi web *E-Government* Dikbud Kota Malang.

3.4 Metode Pengumpulan Data

Dalam penelitian ini, peneliti memilih untuk menggunakan data primer sebagai metode pengambilan data. Alasan utama di balik pilihan ini adalah validitas informasi yang diperoleh lebih akurat dan relevan langsung dari sumbernya. Dalam konteks *Vulnerability Assessment* untuk aplikasi web *E-Government* seperti dikbud.malangkota.go.id, data primer memungkinkan peneliti untuk melakukan pengujian langsung terhadap sistem, sehingga peneliti dapat mengidentifikasi kerentanan dan celah keamanan secara langsung.

3.4.1 Observasi

Melakukan observasi atau pengamatan lansung pada keamanan web Dikbud Kota Malang, melalui url: https://dikbud.malangkota.go.id/.

3.4.2 Wawancara

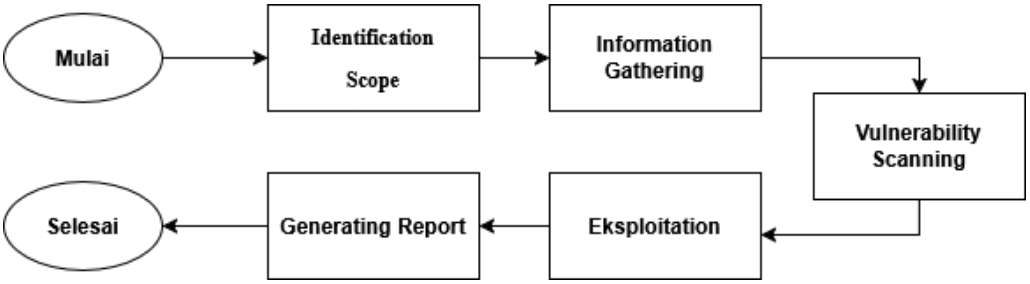
Melakukan proses tanya jawab yang dilakukan secara langsung kepada divisi kebudayaan selaku pengguna dari *website* Dinas Pendidikan Kebudayaan Kota Malang (https://dikbud.malangkota.go.id/).

3.4.3 Eksperimen Lab Komputer

Melakukan pengujian langsung terhadap *website* menggunakan alat keamanan seperti OWASP ZAP. Data yang dihasilkan dari pemindaian ini akan mencakup laporan yang menunjukkan kerentanan yang teridentifikasi, tingkat risiko, dan deskripsi tentang bagaimana kerentanan tersebut dapat dieksploitasi.

3.5 Tahapan Penelitian

Berdasarkan kajian teori yang telah diuraikan sebelumnya, Penelitian ini Melakukan Penelitian dengan menerapkan metode *Vulnerability Assessment* yang berpedoman pada standar *Open Web Application Security Project (OWASP)*. Metode *vulnerability assessment* 5 tahap dipilih karena prosesnya yang lebih sederhana dan efisien, memungkinkan deteksi serta mitigasi celah keamanan utama dengan cepat. Sedangkan PTES 7 tahap menawarkan analisis yang lebih mendetail namun memerlukan waktu dan sumber daya yang lebih banyak. Tahapan yang dilaksanakan adalah *Identification Scope, Information Gathering, Vulnerability Scanning, Eksploitation, Generating Report*. Berikut alur tahapan *vulnerability assesment* yang dilakukan dalam penelitian ini:



Gambar 3.1 Tahapan Penelitian

1. ***Identification Scope***

   Pada tahap ini, peneliti meminta izin penelitian dan mengatur ruang lingkup batasan pengujian untuk memastikan bahwa pengujian hanya mencakup area yang relevan dengan tujuan evaluasi keamanan situs web.

2. ***Information Gathering***

   Tahap pengumpulan informasi bertujuan untuk mengidentifikasi teknologi yang digunakan oleh *website*, termasuk *server*, platform, dan layanan pendukung. Alat yang digunakan dalam tahap ini meliputi *Whois* untuk memperoleh informasi *domain*, Zenmap untuk pemetaan jaringan.

3. ***Vulnerability Scanning***

   Proses pemindaian kerentanan memanfaatkan OWASP ZAP guna mendeteksi kemungkinan adanya celah keamanan pada situs web.

4. **Eksploitasi**

   Tahap ini memanfaatkan OWASP ZAP, bertujuan untuk memverifikasi apakah celah keamanan yang ditemukan dapat dieksploitasi oleh penyerang.

5. ***Generating Report***

   Laporan akhir disusun berdasarkan hasil temuan, mencakup tingkat risiko, serta rekomendasi solusi yang diperlukan untuk meningkatkan keamanan *website*.

3.6 Pengujian Sistem

Dikarenakan keterbatasan waktu dan informasi dari penumpulan data, penelitian ini menggunakan metode *Black-box Testing*. Dalam konteks *Penetration Testing*, *Black-box Testing* mensimulasikan serangan dari perspektif penyerang yang tidak mengetahui detail sistem, yang memungkinkan identifikasi kerentanan yang dapat dieksploitasi dari luar. Penguji hanya berfokus pada input dan output, mengevaluasi apakah *website* berfungsi seperti yang diharapkan.

3.7 Alat Penelitian

3.7.1 Whois

Pada penelitian ini, peneliti memanfaatkan *Whois* untuk mengetahui data atau informasi tentang suatu *domain* tertentu. Layanan ini menyediakan dan menampilkan informasi kepemilikan *domain*, misalnya nama pemilik, kontak, alamat, dan sebagainya.

3.7.2 Zenmap

Pada penelitian ini, peneliti memanfaatkan perangkat lunak Zenmap. Merupakan sebuah aplikasi *open-source* untuk explorasi network dan audit keamanannya. Untuk melakukan *scanning,* peneliti akan menggunakan profil *Intense scan*.

3.7.3OWASP ZAP

Pada penelitian ini, peneliti memanfaatkan perangkat lunak OWASP ZAP (*Zed Attack Proxy*), merupakan alat pemindai keamanan aplikasi web yang bersifat *open-source* dan gratis. Alat ini dirancang untuk membantu pengembang menemukan dan memperbaiki kerentanan keamanan dalam aplikasi web.

BAB IV
HASIL DAN PEMBAHASAN

4.1 Deskripsi Umum Penelitian

Penelitian ini melibatkan *website* https://dikbud.malangkota.go.id/ oleh Dinas Pendidikan dan Kebudayaan Kota Malang. Pemerintah Kota Malang melalui Dinas Pendidikan dan Kebudayaan Kota Malang menyediakan pelayanan publik untuk mempermudah masyarakat khususnya para pelaku akademik pendidikan dasar, pelaku seni atau organisasi pendidikan dan kebudayaan yang ada di Kota Malang. Layanan online nya sendiri mencangkup urusan legalisir, mengajukan kenaikan pangkat guru, mutasi siswa, sampai pembuatan Kartu Induk Kesenian.

Penelitian ini dilakukan dengan menggunakan metode *Vulnerability Assessment*, metode *vulnerability assessment* 5 tahap dipilih karena prosesnya yang lebih sederhana dan efisien, tahapan yang dilaksanakan adalah *Identification Scope*, *Information Gathering*, *Vulnerability Scanning*, *Eksploitation*, *Generating Report,* untuk melakukan pengujian kerentanan menggunakan *tools Whois,* Zenmap, OWASP ZAP, pada *website* yang diuji.

4.2 Peralatan *Software* dan *Hardware*

4.2.1 Perangkat *Software*

Adapun instrumen *Software* yang penulis gunakan dalam penelitian ini adalah:

1. Sistem Operasi *Windows 10*.
2. *Browser Mozilla.*
3. *Software Penetration Testing* seperti Zenmap, OWASP ZAP, *Whois lookup.*

4.2.2 Perangkat *Hardware*

Adapun instrumen *Hardware* yang digunakan dalam penelitian ini adalah laptop dengan spesifikasi sebagai berikut:

1. *Processor: I5-6198du (4 Core)*
2. *RAM: 4GB 2133mhz*
3. *VGA: Intel UHD & NVIDIA MX930 2GB*
4. *Storage: SSD Sata 128GB*
5. *Networking: LAN 1Gb, WIFI 5 (2,4Ghz), Bluetooth.*

4.3 Tahapan Analisis Penelitian

4.3.1 *Identification Scope*

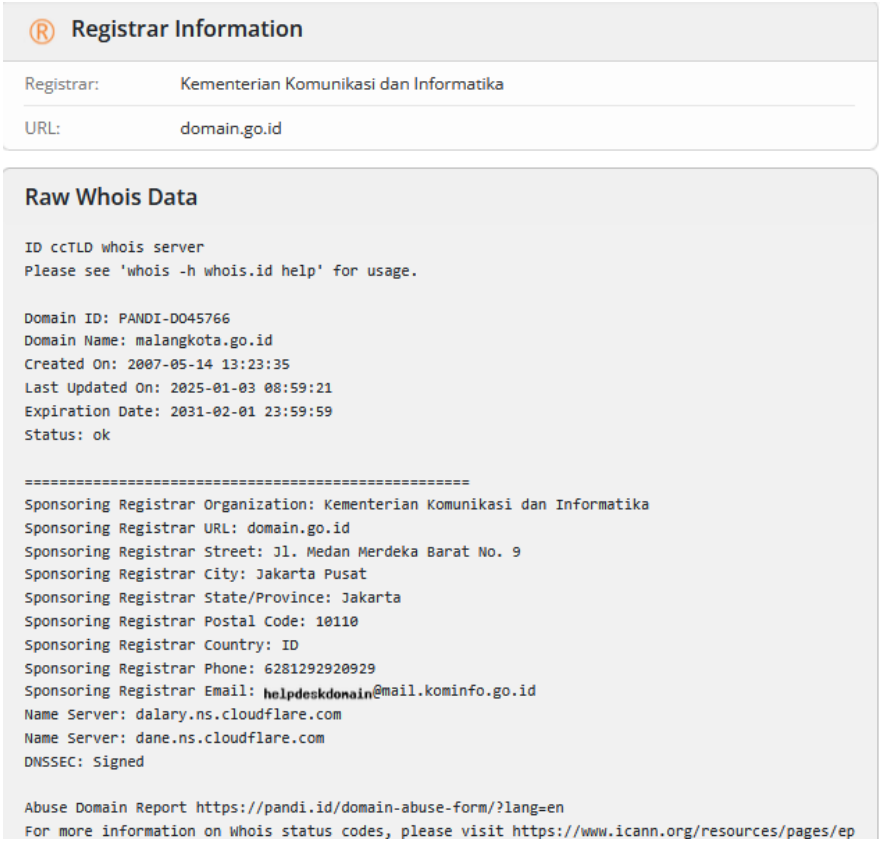
Pada tahapan ini, peneliti meminta izin kepala Dinas Pendidikan dan Kebudayaan Kota Malang untuk melakukan penelitian *Penetration Testing* terhadap *website* https://dikbud.malangkota.go.id/ Adapun surat izin penelitian dapat dilihat pada lampiran penelitian.

4.3.2 *Information Gathering*

Pada tahapan *Information Gathering* dilakukan pengumpulan informasi terhadap *website* https://dikbud.malangkota.go.id/, pengumpulan informasi dilakukan menggunakan *tools Whois* dan Zenmap.

4.3.2.1 Whois

Hasil yang didapatkan dari scanning menggunakan Whois menunjukkan informasi penting mengenai pendaftaran domain, termasuk pemilik, kontak, dan tanggal kedaluwarsa. Berikut adalah rincian hasil *scanning* Whois:



Registrar Information

Registrar:	Kementerian Komunikasi dan Informatika
URL:	domain.go.id

Raw Whois Data

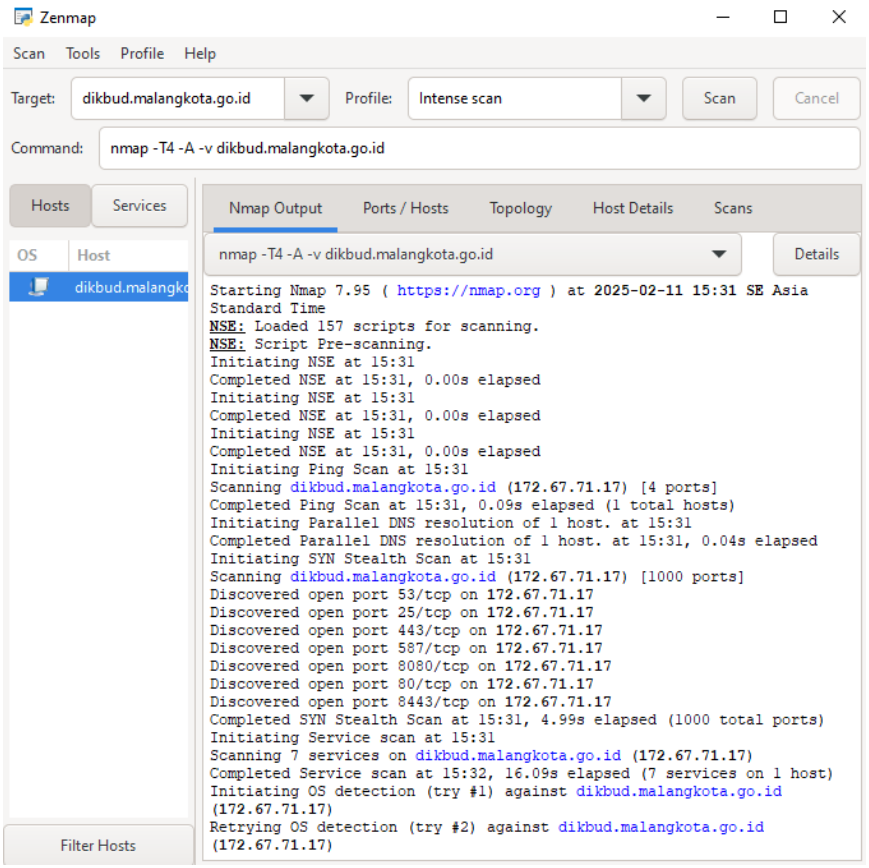
```
ID ccTLD whois server
Please see 'whois -h whois.id help' for usage.

Domain ID: PANDI-DO45766
Domain Name: malangkota.go.id
Created On: 2007-05-14 13:23:35
Last Updated On: 2025-01-03 08:59:21
Expiration Date: 2031-02-01 23:59:59
Status: ok

==================================================
Sponsoring Registrar Organization: Kementerian Komunikasi dan Informatika
Sponsoring Registrar URL: domain.go.id
Sponsoring Registrar Street: Jl. Medan Merdeka Barat No. 9
Sponsoring Registrar City: Jakarta Pusat
Sponsoring Registrar State/Province: Jakarta
Sponsoring Registrar Postal Code: 10110
Sponsoring Registrar Country: ID
Sponsoring Registrar Phone: 6281292920929
Sponsoring Registrar Email: helpdeskdomain@mail.kominfo.go.id
Name Server: dalary.ns.cloudflare.com
Name Server: dane.ns.cloudflare.com
DNSSEC: Signed

Abuse Domain Report https://pandi.id/domain-abuse-form/?lang=en
For more information on Whois status codes, please visit https://www.icann.org/resources/pages/ep
```

Gambar 4.1 Hasil Pengecekan *Whois*

Berdasarkan data *Whois* dari *domain* https://dikbud.malangkota.go.id/ merupakan *sub-domain* dari malangkota.go.id, *IP (Internet Protocol) Address* yang digunakan adalah 172.67.71.17, status *domain* tersebut adalah aman. *Domain* ini terdaftar di Kementerian Komunikasi dan Informatika pada tanggal 14 Mei 2007 dan masih memiliki masa *expired* sampai tanggal 1 Februari 2031. Selain itu, *domain* ini juga menggunakan DNSSEC, fitur keamanan yang melindungi dari pemalsuan DNS.

4.3.2.2 Zenmap

Hasil yang didapatkan dari hasil *Scanning* menggunkan *profile Intense Scan* dengan perintah nmap -T4 -A -v https://dikbud.malangkota.go.id/ sebagai berikut:



Gambar 4.2 Hasil *Scan* Zenmap

Berdasarkan hasil *scan* Zenmap, diketahui bahwa *IP Address* yang digunakan oleh *website* https://dikbud.malangkota.go.id/ adalah 172.67.71.17. *Server* tersebut di hosting pada penyedia layanan *cloud* atau data center menggunakan layanan *Cloudflare* sebagai *reverse proxy* dan CDN (*Content Delivery Network*). Terdapat juga *port-port* yang terbuka (dapat disusupi). Berikut hasil *scan* dalam bentuk table:

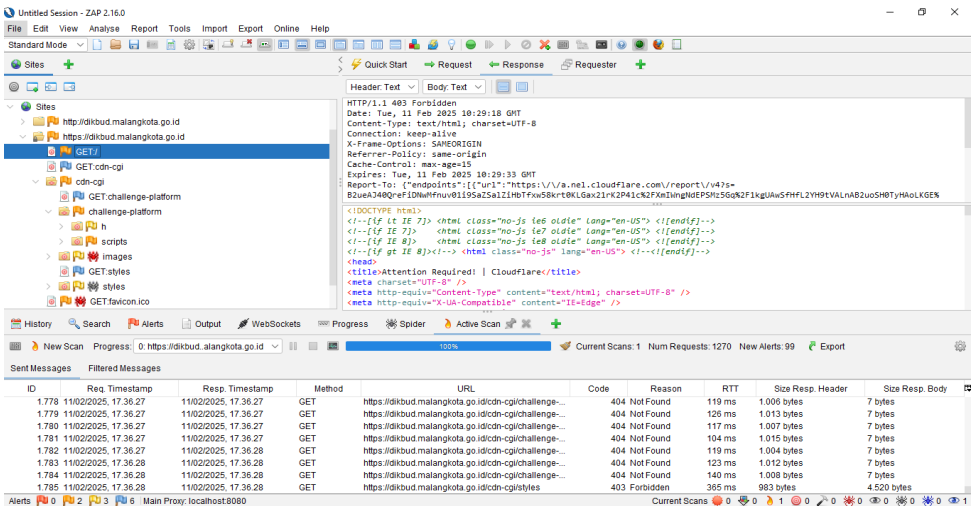
Tabel 4.1 Hasil *Scanning* Zenmap

Hasil *Scanning*	**Keterangan**
Server	*Cloudflare*
Platform	*Cloudflare*
Port TCP/25 on 172.67.71.17	*Open*

Port TCP/53 on 172.67.71.17	*Open*
Port TCP/80 on 172.67.71.17	*Open*
Port TCP/443 on 172.67.71.17	*Open*
Port TCP/587 on 172.67.71.17	*Open*
Port TCP/8080 on 172.67.71.17	*Open*
Port TCP/8443 on 172.67.71.17	*Open*

4.3.3 *Vulnerabillity Scanning*

Dalam tahapan ini alat yang digunakan adalah OWASP ZAP. Berikut proses *scan* OWASP ZAP:



Gambar 4.3 Proses *Scan* OWASP ZAP

Setelah melakukan penetrasi selama 5 menit menggunakan *tools* OWASP ZAP, terdapat berbagai resiko kerentanan yang terdeteksi dalam aplikasi web, berikut merupakan tabel hasil *scanning* OWASP ZAP:

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	1 (9.1%)	1 (9.1%)	0 (0.0%)	2 (18.2%)
	Low	0 (0.0%)	1 (9.1%)	1 (9.1%)	1 (9.1%)	3 (27.3%)
	Informational	0 (0.0%)	0 (0.0%)	3 (27.3%)	3 (27.3%)	6 (54.5%)
	Total	0 (0.0%)	2 (18.2%)	5 (45.5%)	4 (36.4%)	11 (100%)

Gambar 4.4 Hasil *Scan* OWASP ZAP

Hasil penetrasi OWASP ZAP menunjukkan total 11 temuan kerentanan. Sebagian besar temuan (54.5%) dikategorikan sebagai risiko "Informational", dengan tingkat kepercayaan "*Medium*" dan "*Low*". Terdapat 2 temuan berisiko "*Medium*" dan 3 temuan berisiko "*Low*", sementara tidak ada temuan berisiko "*High*". Ini menunjukkan bahwa meskipun terdapat beberapa kerentanan, mayoritas tidak memiliki dampak kritis terhadap sistem. Berikut jenis *alert* dan *level* resiko dalam bentuk tabel:

Tabel 4.2 Daftar Kerentanan

No.	***Alert***	***Risk***
1	*Content Security Policy (CSP) Header Not Set*	*Medium*
2	*Cross-Domain Misconfiguration*	*Medium*
3	*Cookie with Same-Site Attribute None*	*Low*
4	*Strict-Transport-Security Header Not Set*	*Low*
5	*Timestamp Disclosure – Unix*	*Low*
6	*Session Management Response Identified*	*Informational*
7	*Loosely Scoped Cookie*	*Informational*
8	*Information Disclosure – Suspicious Comment*	*Informational*
9	*Retrieved from Cache*	*Informational*
10	*Re-examine Cache-control Directives*	*Informational*
11	*User Agent Fuzzer*	*Informational*

4.3.4 *Exploitation*

Hasil pengujian *Scanning* OWASP menunjukkan bahwa tidak ada celah keamanan tingkat tinggi. Sehingga, tidak memiliki dampak kritis terhadap sistem. Dapat dilihat dalam hasil berikut:

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://dikbud.malangkota.go.id	0 (0)	2 (2)	3 (5)	6 (11)

Gambar 4.5 Hasil Penetrasi OWASP ZAP

4.3.5 *Generating Report*

Pada tahapan ini semua data dari hasil pengujian dikumpulkan menjadi sebuah laporan. Adapun laporan terhadap pengujian *website* https://dikbud.malangkota.go.id/ adalah sebagai berikut:

1. Hasil Pengumpulan data melalui *Scanning Whois* yaitu sebagai berikut:

Tabel 4.3 Hasil *Scanning Whois*

Hasil Scanning	**Keterangan**
Domain Utama	https://malangkota.go.id/
Nama *Sub-domain*	https://dikbud.malangkota.go.id/
IP Address	*172.67.71.17*
Tanggal Registrasi	14-05-2007
Tanggal Berakhir	01-02-2031

2. Hasil Pengumpulan data melalui *Scanning* menggunakan Zenmap yaitu didapatkan detail *server* sebagai berikut:

Tabel 4.4 Hasil *Scanning* Zenmap

Hasil *Scanning*	**Keterangan**
Server	*Cloudflare*
Platform	*Cloudflare*
Port TCP/25 on 172.67.71.17	*Open*
Port TCP/53 on 172.67.71.17	*Open*
Port TCP/80 on 172.67.71.17	*Open*
Port TCP/443 on 172.67.71.17	*Open*
Port TCP/587 on 172.67.71.17	*Open*
Port TCP/8080 on 172.67.71.17	*Open*
Port TCP/8443 on 172.67.71.17	*Open*

3. Hasil Pengujian *Scanning* menggunakan OWASP didapatkan beberapa kerentanan pada beberapa tingkatan yaitu sebagai berikut:

Tabel 4.5 Daftar Kerentanan

No.	***Alert***	***Risk***
1	*Content Security Policy (CSP) Header Not Set*	*Medium*
2	*Cross-Domain Misconfiguration*	*Medium*
3	*Cookie with Same-Site Attribute None*	*Low*
4	*Strict-Transport-Security Header Not Set*	*Low*
5	*Timestamp Disclosure – Unix*	*Low*
6	*Session Management Response Identified*	*Informational*
7	*Loosely Scoped Cookie*	*Informational*
8	*Information Disclosure – Suspicious Comment*	*Informational*
9	*Retrieved from Cache*	*Informational*
10	*Re-examine Cache-control Directives*	*Informational*
11	*User Agent Fuzzer*	*Informational*

Terdapat 11 kerentanan yang didapatkan oleh OWASP ZAP yaitu 2 pada *level medium*, pada *level low* ditemukan 3, dan 6 informasi saran perbaikan. Dapat disimpulkan berdasarkan hasil pengujian OWASP ZAP *website* hanya memiliki kerentanan di *level low* sehingga *website* cukup aman dan hanya dibutuhkan beberapa penyesuaian saja.

4. Hasil pengujian *Exploitation* OWASP menunjukkan bahwa tidak ada celah keamanan tingkat tinggi. Sehingga, tidak memiliki dampak kritis terhadap system.

Dari semua hasil pengujian yang telah dilakukan maka dapat disimpulkan bahwa website https://dikbud.malangkota.go.id/ sudah termasuk aman hanya saja perlu dilakukan beberapa penyesuaian yang ditemukan oleh OWASP agar keamanan website lebih meningkat lagi.

4.4 Pengujian Sistem

Dalam pengujian penetrasi situs web menggunakan metode *Black-box Testing* dengan *tools* OWASP ZAP, penguji berperan sebagai penyerang eksternal. Hasil dari pengujian mengidentifikasi kerentanan seperti formulir HTML tanpa perlindungan *CSRF* (*Cross-Site Request Forgery*) yang merupakan pemalsuan permintaan lintas situs dan *Clickjacking*.

Kerentanan *CSRF* (*Cross-Site Request Forgery*) terjadi ketika situs web tidak memiliki mekanisme perlindungan pada formulirnya, sehingga hacker bisa mengeksploitasi pengguna untuk melakukan tindakan tanpa izin, seperti mengganti kata sandi atau melakukan transaksi. Sementara itu, *Clickjacking* terjadi ketika situs tidak memiliki pengaturan keamanan yang mencegah tampilan dalam *frame*

halaman situs web, sehingga hacker dapat menipu pengguna agar mengklik sesuatu tanpa sadar.

4.5 Pembahasan

4.5.1 *Content Security Policy (CSP) Header Not Set*

Temuan pertama pada situs web https://dikbud.malangkota.go.id/ adalah tipe *alert level medium* yaitu *Content Security Policy (CSP) Header Not Set* yang artinya belum menerapkan *Content Security Policy (CSP),* yang merupakan mekanisme esensial dalam melindungi aplikasi web dari serangan injeksi code. (Dedi Supriadi, dkk. 2024) merekomendasikan solusi mengkonfigurasi *CSP (Content Security Policy)* untuk membatasi sumber daya yang diizinkan untuk dimuat oleh *browser*.

4.5.2 *Cross-Domain Misconfiguration*

Temuan kedua pada situs web https://dikbud.malangkota.go.id/ adalah tipe *alert level medium* yaitu *Cross-Domain Misconfiguration* yang artinya terdapat pemuatan data web *browser* dimungkinkan karena kesalahan konfigurasi *CORS* (akses sumber daya terbatas antar domain di *server* web), Menurut (Riyan Farismana,dkk. 2023) solusinya hapus semua *header Cross Origin Resource Sharing (CORS)* agar *browser* menerapkan kebijakan yang sama dengan cara yang lebih ketat.

4.5.3 *Cookie with Same-Site Attribute None*

Temuan ketiga pada situs web https://dikbud.malangkota.go.id/ adalah tipe *alert level low* yaitu *Cookie with Same-Site Attribute None* yang artinya terdapat atribut *Same-Site=None* pada *cookie* memungkinkan *hacker* mengirim *cookie* lintas situs yang diperlukan untuk fungsionalitas seperti integrasi pihak ketiga dan

autentikasi lintas *domain*. Menurut (Riyan Farismana, dkk. 2023) solusinya adalah dengan selalu menggunakan atribut Secure (HTTPS), memvalidasi dan membersihkan *input*, dan menggunakan *token CSRF*.

4.5.4 *Strict-Transport-Security Header Not Set*

Temuan keempat pada situs web https://dikbud.malangkota.go.id/ adalah tipe *alert level low* yaitu *Strict-Transport-Security Header Not Set* yang artinya ketiadaan *Header Strict Transport Security (HSTS)* pada situs web Dinas Pendidikan dan Kebudayaan Kota Malang menunjukkan bahwa situs tersebut belum memastikan penggunaan protokol HTTPS secara konsisten dalam komunikasi. Menurut (Riyan Farismana, dkk. 2023) solusinya pastikan bahwa *server* web, *server* aplikasi*, load balance* dikonfigurasi untuk menerapkan *Strict-Transport-Security.*

4.5.5 *Timestamp Disclosure – Unix*

Temuan kelima pada situs web https://dikbud.malangkota.go.id/ adalah tipe *alert level low* yaitu *Timestamp Disclosure – Unix* yang artinya berdasarkan analisis terhadap *website*, pengungkapan *Timestamp – Unix* dalam aplikasi web dapat mengungkapkan informasi waktu, pada sistem *server*, yang berpotensi dimanfaatkan oleh penyerang untuk melancarkan serangan atau mengidentifikasi versi perangkat lunak yang digunakan. Menurut (Dedi Supriadi, dkk. 2024) solusinya menyembunyikan atau meminimalisir informasi terkait *Timestamp* untuk mengurangi potensi eksploitasi.

4.5.6 *Session Management Response Identified*

Temuan keenam pada situs web https://dikbud.malangkota.go.id/ adalah tipe *alert level informational* yaitu *Session Management Response Identified* yang

artinya respons dari *server* web mengandung *token* manajemen sesi, peringatan ini tidak menunjukkan adanya kerentanan, tetapi memberikan informasi bahwa *token* sesi telah terdeteksi dalam *respons* tersebut.

Menurut Johns et al. (2010) untuk mengatasi masalah ini, disarankan untuk menerapkan praktik manajemen sesi yang kuat, seperti penggunaan pengidentifikasi sesi yang aman dan acak, pengaturan waktu kedaluwarsa sesi yang tepat, dan implementasi mekanisme logout yang efektif.

4.5.7 *Loosely Scoped Cookie*

Temuan ketujuh pada situs web https://dikbud.malangkota.go.id/ adalah tipe *alert level informational* yaitu *Loosely Scoped Cookie* yang artinya terdapat *cookie* dengan cakupan *domain* yang longgar dapat menyebabkan kerentanan keamanan, seperti injeksi *cookie* dari satu *domain* ke *domain* yang terkait lainnya.

Menurut Zheng et al. (2015) untuk mengatasi masalah ini, disarankan untuk menetapkan cakupan *cookie* secara spesifik pada *sub-domain* yang diperlukan dan menghindari penggunaan cakupan *domain* yang terlalu luas.

4.5.8 *Information Disclosure – Suspicious Comment*

Temuan kedelapan pada situs web https://dikbud.malangkota.go.id/ adalah tipe *alert level informational* yaitu *Information Disclosure – Suspicious Comment* yang artinya komentar dalam kode sumber situs web https://dikbud.malangkota.go.id/ terdeteksi dan dapat mengungkapkan informasi tambahan terkait aplikasi web. (Dedi Supriadi, dkk. 2024) Merekomendasikan solusi hapus komentar kode yang yang mengandung informasi sensitif pada aplikasi web.

4.5.9 *Retrieved from Cache Informational*

Temuan kesembilan pada situs web https://dikbud.malangkota.go.id/ adalah tipe *alert level informational* yaitu *Retrieved from Cache Informational* yang artinya *cache* yang tidak terkonfigurasi dengan baik. Menurut (Haeruddin dan Hermanto, 2022) untuk mengatasi masalah ini, disarankan untuk mengatur kode header HTTP dengan benar, seperti *Cache-Control: no-store* atau *Cache-Control: private*, untuk memastikan bahwa informasi sensitif tidak disimpan dalam cache bersama.

4.5.10 *Re-examine Cache-control Directives*

Temuan kesepuluh pada situs web https://dikbud.malangkota.go.id/ adalah tipe *alert level informational* yaitu *Re-examine Cache-control Directives* yang artinya kesalahan dalam pengaturan kontrol *cache* pada situs web yang dapat menyebabkan penyimpanan data sensitif di dalam *cache*. (Dedi Supriadi, dkk. 2024) merekomendasikan solusi optimalkan direktif *cache-control* untuk mencegah penyimpanan data sensitif pada klien.

4.5.11 *User Agent Fuzzer*

Temuan kesebelas pada situs web https://dikbud.malangkota.go.id/ adalah tipe *alert level informational* yaitu *User Agent Fuzzer* yang artinya penggunaan *tools fuzzing* (menguji *respons website* terhadap manipulasi parameter) yang tidak efektif pada *Header User-Agent* pada situs web https://dikbud.malangkota.go.id/. (Dedi Supriadi, dkk. 2024) merekomendasikan solusi periksa kembali autentikasi pengguna dan proses identifikasi untuk mencegah eksploitasi melalui *fuzzing.*

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil *Vulnerability Assessment* pada situs web Dinas Pendidikan dan Kebudyaan Kota Malang, untuk mengetahui celah keamanan yang dilakukan pada aplikasi web *E-Government* pada tahap *Information Gathering* menemukan beberapa informasi diantaranya *ip address, port-open, server host*, lokasi, serta *domain* yang diuji. Kemudian tahapan *Vulnerability Scanning* ditemukan total 11 kerentanan yang terdiri dari 2 vulnerabilitas yang memiliki risiko menengah, 3 vulnerabilitas yang memiliki risiko rendah, serta 6 vulnerabilitas informatif. Secara keseluruhan, meskipun aspek keamanan sudah cukup terjaga, perbaikan lebih lanjut tetap diperlukan, terutama untuk menangani kerentanan dengan risiko menengah.

Pada tahap akhir tahap pendokumentasian risiko dengan spesifikasi deskripsi kerentanan dan solusi yang dapat diterapkan untuk memperbaiki celah kerentanan pada aplikasi web *E-Government* Dinas Pendidikandan Kebudayaan Kota Malang.

5.2 Saran

Berdasarkan pengujian pada BAB sebelumnya, maka meneliti menyarankan:

1. Untuk pengujian selanjutnya diharapkan menggunakan *Framework* yang berbeda seperti *BurpSuite* atau ISSAF (*Information System Security Assesment Framework*).
2. Disarankan untuk Dinas Pendidikan dan Kebudayaan Kota Malang memperbaiki kerentanan sistem pada *level medium* dan *low* serta informasi perbaikan yang disarankan OWASP untuk meningkatkan keamanan *website*.

DAFTAR PUSTAKA

Al-Shboul, M. A., Abourdaha, S., & Shah, M. 2018. *Web penetration testing: Tools, methodologies, and ethics*. International Journal of Computer Science and Network Security, 18(5), 123-135.

Andhika. 2023. *Mengenal Vulnerability Assessment and Penetration Testing (VAPT): Apa itu dan Mengapa Penting?* Fourtrezz. Retrieved from https://fourtrezz.co.id

Appiah, A. A., Kusi-Sarpong, S., Danquah, E., & Boateng, F. 2019. *Web application security: An overview of OWASP top 10 security risks*. International Journal of Cyber Security and Digital Forensics, 8(2), 45-61.

Budiman, A., Wijaya, R., & Setiawan, B. 2021. *Implementasi metode Vulnerability Assessment and Penetration Testing (VAPT) dalam pengujian keamanan aplikasi web*. Jurnal Teknologi dan Keamanan Informasi, 9(1), 1-10.

Candra Darmawan, A., Putra, F. D., & Wibowo, A. 2024. *Penerapan metode Vulnerability Assessment untuk identifikasi keamanan website berdasarkan OWASP ID Tahun 2021*. Jurnal Keamanan Informasi dan Teknologi, 12(3), 100-115.

Dedi Supriadi, Suryadi, E., Muslim, R., & Samsumar, L. D. 2024. *Implementasi vulnerability assessment OWASP (Open Web Application Security Project) pada website Universitas Teknologi Mataram*. Jurnal Sistem Informasi dan Keamanan Data, 11(2), 45-60.

Desty Luthfiani. 2024. *Peretasan Pusat Data Nasional Sementara, website Kemendikbud jadi korban*. Tempo.co. Retrieved from https://www.tempo.co

Farismana, R., & Pramadhana, D. 2023. *Vulnerability Assessment untuk analisis tingkat keamanan pada sistem informasi repositori karya ilmiah Politeknik XYZ*. Jurnal Manajemen Informatika & Sistem Informasi, 6(1), 45-59.

Hafitzhah, N., Surya, M., & Rachmat, A. 2023. *Analisis keamanan sistem informasi berbasis web dengan metode penetration testing*. Jurnal Teknologi dan Keamanan Siber, 11(2), 30-45.

Haeruddin, M., & Hermanto, A. 2022. *Optimalisasi keamanan aplikasi web menggunakan metode OWASP ZAP*. Jurnal Keamanan Data dan Informasi, 10(4), 88-105.

Ibrahim, R., & Khan, M. 2016. *The evolution of websites: A historical perspective and future trends*. Journal of Web Technology and Development, 7(3), 121-135.

Johns, M., Smith, T., & Brown, R. 2010. *Secure session management: Techniques and best practices*. International Journal of Web Security, 5(2), 78-92.

Johnston, M. P., & Becker, L. 2020. *The role of experimental case study in cybersecurity research*. Journal of Information Security and Applications, 54, 102525.

Kaur, P., & Kaur, H. 2019. *Cybersecurity threats and risk assessment in digital era*. International Journal of Cybersecurity and Intelligence, 8(1), 55-72.

Khan, M., Patel, R., & Verma, S. 2019. *Grey-box testing methodologies in penetration testing: A hybrid approach*. Journal of Cybersecurity Research, 6(3), 112-128.

Leszczyna, R. 2021. *White-box security testing for web applications: A comparative analysis*. Journal of Web Engineering and Security, 12(1), 25-41.

Maia, J., & D'Ambrosio, L. 2020. *Black-box testing in web applications: Techniques, challenges, and solutions*. Journal of Software Engineering Research and Development, 8(2), 67-83.

Martinez, F., & Zhao, L. 2021. *Experimental case studies in cybersecurity research: Bridging the gap between academia and industry*. Cybersecurity and Data Privacy Journal, 9(3), 152-170.

Nur Cholifah. 2018. *Pengujian sistem perangkat lunak dengan pendekatan black-box testing*. Jurnal Rekayasa Perangkat Lunak, 5(2), 35-50.

Nurul Huda. 2022. *Apa itu WHOIS, cara kerja, hingga fungsinya untuk domain*. Retrieved from https://www.dewaweb.com/blog

Riskiyadi, M., Anggono, A., & Tarjo. 2021. *Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis*. Jurnal Manajemen dan Organisasi.

Riyan Farismana, & Pramadhana, D. 2023. *OWASP ZAP sebagai alat untuk mendeteksi kerentanan aplikasi web*. Jurnal Keamanan Siber dan Teknologi, 5(1), 15-30.

Syarif, T. R. 2019. *Analisis Perbandingan Metode Web Security PTES, ISSAF Dan OWASP di Dinas Komunikasi Dan Informasi Kota* (Doctoral dissertation, Universitas Komputer Indonesia).

Verma, S., & Sharma, P. 2017. *Penetration testing tools: An overview and comparative study*. Journal of Cybersecurity Technologies, 4(1), 88-102.

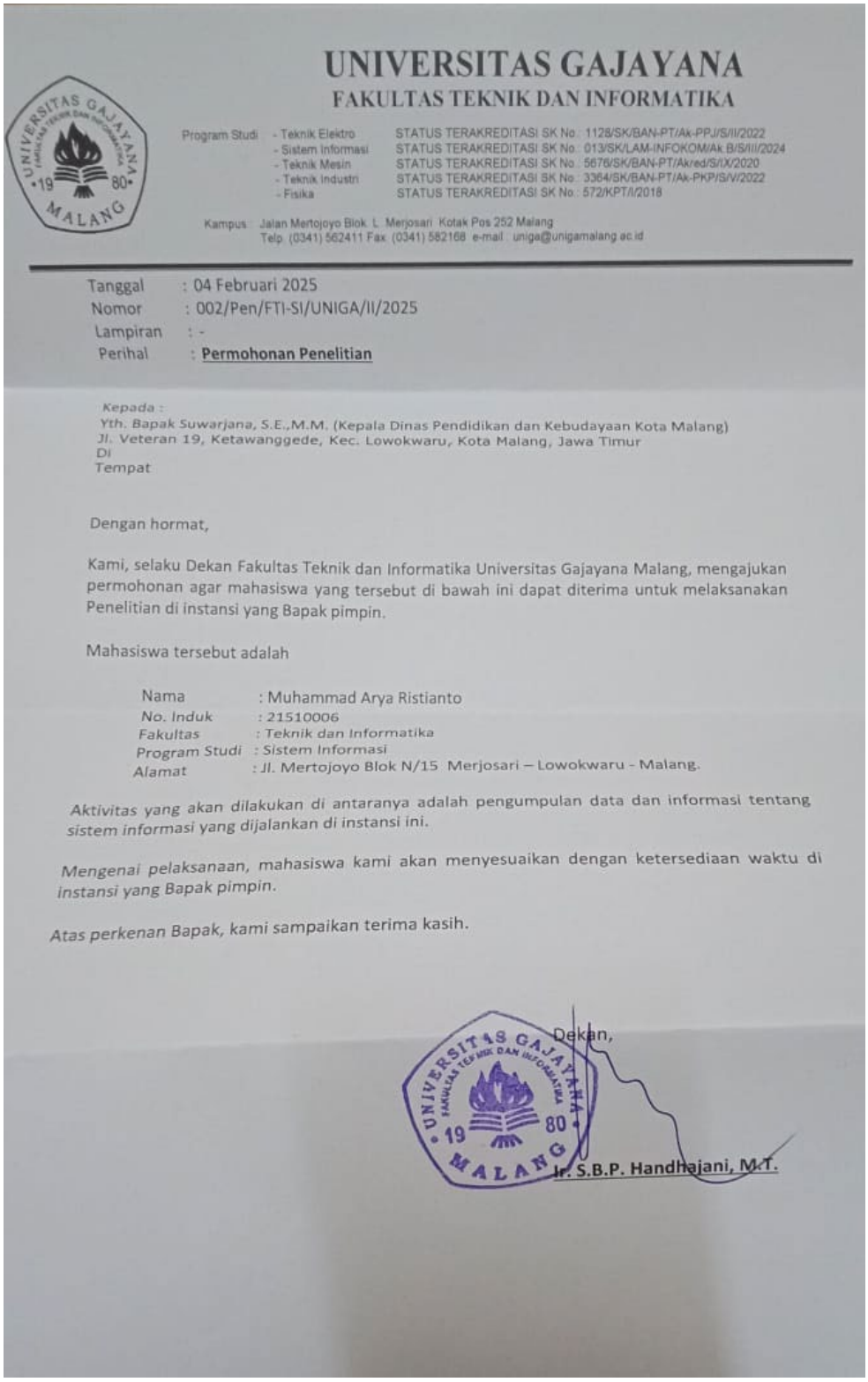
Wijayanti, N. N. 2022. *Pengertian website lengkap dengan jenis dan manfaatnya*. Retrieved from https://www.niagahoster.co.id/blog

Zheng, L., Xu, Y., & Wang, H. 2015. *Web security: Best practices for cookie management and data protection*. Journal of Web Security and Development, 10(4), 95-112.

LAMPIRAN

Lampiran 1

Surat pengantar dan surat izin melakukan penelitian



UNIVERSITAS GAJAYANA
FAKULTAS TEKNIK DAN INFORMATIKA

Program Studi
- Teknik Elektro — STATUS TERAKREDITASI SK No.: 1128/SK/BAN-PT/Ak-PPJ/S/II/2022
- Sistem Informasi — STATUS TERAKREDITASI SK No.: 013/SK/LAM-INFOKOM/Ak.B/S/II/2024
- Teknik Mesin — STATUS TERAKREDITASI SK No.: 5676/SK/BAN-PT/Akred/S/IX/2020
- Teknik Industri — STATUS TERAKREDITASI SK No.: 3364/SK/BAN-PT/Ak-PKP/S/V/2022
- Fisika — STATUS TERAKREDITASI SK No.: 572/KPT/I/2018

Kampus : Jalan Mertojoyo Blok L Merjosari Kotak Pos 252 Malang
Telp. (0341) 562411 Fax. (0341) 582168 e-mail : uniga@unigamalang.ac.id

Tanggal : 04 Februari 2025
Nomor : 002/Pen/FTI-SI/UNIGA/II/2025
Lampiran : -
Perihal : **Permohonan Penelitian**

Kepada :
Yth. Bapak Suwarjana, S.E.,M.M. (Kepala Dinas Pendidikan dan Kebudayaan Kota Malang)
Jl. Veteran 19, Ketawanggede, Kec. Lowokwaru, Kota Malang, Jawa Timur
Di
Tempat

Dengan hormat,

Kami, selaku Dekan Fakultas Teknik dan Informatika Universitas Gajayana Malang, mengajukan permohonan agar mahasiswa yang tersebut di bawah ini dapat diterima untuk melaksanakan Penelitian di instansi yang Bapak pimpin.

Mahasiswa tersebut adalah

Nama : Muhammad Arya Ristianto
No. Induk : 21510006
Fakultas : Teknik dan Informatika
Program Studi : Sistem Informasi
Alamat : Jl. Mertojoyo Blok N/15 Merjosari – Lowokwaru - Malang.

Aktivitas yang akan dilakukan di antaranya adalah pengumpulan data dan informasi tentang sistem informasi yang dijalankan di instansi ini.

Mengenai pelaksanaan, mahasiswa kami akan menyesuaikan dengan ketersediaan waktu di instansi yang Bapak pimpin.

Atas perkenan Bapak, kami sampaikan terima kasih.

Dekan,

Ir. S.B.P. Handhajani, M.T.

PEMERINTAH KOTA MALANG
DINAS PENDIDIKAN DAN KEBUDAYAAN

Jl. Veteran No. 19 Telp. (0341) 560946, Fax. (0341) 551333
Website : http://dikbud.malangkota.go.id | Email : dikbud@malangkota.co.id
Malang Kode Pos : 65145

REKOMENDASI

Nomor : 000.9.2/142/35.73.401/2025

Menindaklanjuti surat Dekan Fakultas Teknik dan Informatika Universitas Gajayana Malang dari tanggal 4 Februari 2025 Nomor : 002/Pen/FTI-SI/UNIGA/II/2025 Perihal : Permohonan Izin Penelitian, maka dengan ini Dinas Pendidikan dan Kebudayaan Kota Malang memberi ijin untuk melaksanakan kegiatan dimaksud kepada Saudara :

1. Nama : Muhammad Arya Ristianto
2. NIM : 21510006
3. Jenjang : S1
4. Prodi. / Jurusan : Sistem Informasi
5. Tempat Pelaksanaan : Dinas Pendidikan dan Kebudayaan Kota Malang
6. Waktu Pelaksanaan : 4 Desember 2024 - 4 Februari 2025
7. Judul : Metode vurneralibility Assessment pada Aplikasi Web E-government

Dengan Ketentuan :

1. Dikoordinasikan sebaik – baiknya dengan Kepala Bidang Pembinaan Pendidikan Dasar dan Kepala Dinas Pendidikan dan Kebudayaan Kota Malang
2. Tidak melakukan penelitian yang tidak sesuai atau tidak ada kaitannya dengan judul, maksud dan tujuan penelitian
3. Menjaga perilaku dan menaati tata tertib yang berlaku pada lembaga tersebut di atas;
4. Menaati ketentuan peraturan perundang-undangan;
5. Selesai melaksanakan penelitian / Observasi / KKL / KKN, wajib menyampaikan laporan kepada Kepala Dinas Pendidikan dan Kebudayaan Kota Malang
6. Dilaksanakan dengan tetap memperhatikan protokol kesehatan

Demikian untuk menjadikan periksa.

Malang, 5 Februari 2025
A.n KEPALA DINAS PENDIDIKAN DAN KEBUDAYAAN,
Kepala Subbag Umum dan Kepegawaian

PEMERINTAH KOTA MALANG
DINAS PENDIDIKAN DAN KEBUDAYAAN

DYAH KUSARINI, S.Si
Penata Tk I III/d
NIP.198109009292005012017

Tembusan :
Yth.

1. Bpk. Kepala Dinas Pendidikan dan Kebudayaan Kota Malang (Sebagai Laporan)
2. Sdr. Kepala Dinas Pendidikan dan Kebudayaan Kota Malang
3. Sdr. Dekan Fakultas Teknik dan Informatika Universitas Gajayana Malang
4. Yang Bersangkutan

Lampiran 2

Laporan hasil uji penetrasi menggunakan OWASP ZAP:

ZAP by Checkmarx Scanning Report

Generated with ZAP on Tue 11 Feb 2025, at 17:47:00 ZAP

Version: 2.16.0

ZAP by Checkmarx

Contents

- About this report
- Report parameters
- Summaries
- Alert counts by risk and confidence
- Alert counts by site and risk
- Alert counts by alert type
- Alerts
- Risk=Medium, Confidence=High (1)
- Risk=Medium, Confidence=Medium (1)
- Risk=Low, Confidence=High (1)

- Risk=Low, Confidence=Medium (1)
- Risk=Low, Confidence=Low (1)
- Risk=Informational, Confidence=Medium (3)
- Risk=Informational, Confidence=Low (3)
- Appendix
- Alert types

About this report

Report parameters Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

https://dikbud.malangkota.go.id

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

Risk levels

Included: High, Medium, Low, Informational
Excluded: None

Confidence levels

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

	Confidence				
	User Confirmed	**High**	**Medium**	**Low**	**Total**
High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
Medium	0 (0.0%)	1 (9.1%)	1 (9.1%)	0 (0.0%)	2 (18.2%)
Low	0 (0.0%)	1 (9.1%)	1 (9.1%)	1 (9.1%)	3 (27.3%)
Informational	0 (0.0%)	0 (0.0%)	3 (27.3%)	3 (27.3%)	6 (54.5%)

Confidence

	User Confirmed	High	Medium	Low	Total
Total	0 (0.0%)	2 (18.2%)	5 (45.5%)	4 (36.4%)	11 (100%)

Risk

Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

Risk

		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://dikbud.malangkota.go.id	0 (0)	2 (2)	3 (5)	6 (11)

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Content Security Policy (CSP) Header Not Set	Medium	3 (27.3%)
Cross-Domain Misconfiguration	Medium	1 (9.1%)
Cookie with SameSite Attribute None	Low	2 (18.2%)
Strict-Transport-Security Header Not Set	Low	4 (36.4%)
Timestamp Disclosure - Unix	Low	5 (45.5%)
Information Disclosure - Suspicious Comments	Informational	4 (36.4%)
Loosely Scoped Cookie	Informational	2 (18.2%)
Re-examine Cache-control Directives	Informational	1 (9.1%)
Retrieved from Cache	Informational	1 (9.1%)
Session Management Response Identified	Informational	2 (18.2%)
User Agent Fuzzer	Informational	99 (900.0%)
Total		11

Alerts

Risk=Medium, Confidence=High (1)

https://dikbud.malangkota.go.id (1)

Content Security Policy (CSP) Header Not Set (1)

▶ GET https://dikbud.malangkota.go.id/

Risk=Medium, Confidence=Medium (1)

https://dikbud.malangkota.go.id (1)

Cross-Domain Misconfiguration (1)

▶ GET https://dikbud.malangkota.go.id/cdn-cgi/challenge-platform/scripts/jsd/main.js

Risk=Low, Confidence=High (1)

https://dikbud.malangkota.go.id (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://dikbud.malangkota.go.id/cdn-cgi/styles/cf.errors.ie.css

Risk=Low, Confidence=Medium (1)

https://dikbud.malangkota.go.id (1)

Cookie with SameSite Attribute None (1)

▶ POST https://dikbud.malangkota.go.id/cdn-cgi/challenge-platform/h/g/jsd/r/0.6061077610477938:1739265126:yNQn3RClcvcNkBN0_V1lmPV_FD9pCgykAjzeIPp5BlQ/910394a2ff79a030

Risk=Low, Confidence=Low (1)

https://dikbud.malangkota.go.id (1)

Timestamp Disclosure - Unix (1)

▶ GET https://dikbud.malangkota.go.id/cdn-cgi/challenge-platform/h/g/scripts/jsd/8a57887573f2/main.js

Risk=Informational, Confidence=Medium (3)

https://dikbud.malangkota.go.id (3)

Retrieved from Cache (1)

▶ GET https://dikbud.malangkota.go.id/robots.txt

Session Management Response Identified (1)

▶ POST https://dikbud.malangkota.go.id/cdn-cgi/challenge-platform/h/g/jsd/r/0.6061077610477938:1739265126:yNQn3RClcvcNkBN0_

User Agent Fuzzer (1)

▶ GET https://dikbud.malangkota.go.id/

Risk=Informational, Confidence=Low (3)

https://dikbud.malangkota.go.id (3)

Information Disclosure - Suspicious Comments (1)

◀ GET https://dikbud.malangkota.go.id/cdn-cgi/challenge-platform/h/g/scripts/jsd/8a57887573f2/main.js

Loosely Scoped Cookie (1)

◀ POST https://dikbud.malangkota.go.id/cdn-cgi/challenge-platform/h/g/jsd/r/0.6061077610477938:1739265126:yNQn3RClcvcNkBN0_V1lmPV_FD9pCgykAjzeIPp5BlQ/910394a2ff79a030

Re-examine Cache-control Directives (1)

◀ GET https://dikbud.malangkota.go.id/robots.txt

Appendix

Alert types

This section contains additional information on the types of alerts in the report.

Content Security Policy (CSP) Header Not Set **Source** raised by a passive scanner (Content Security Policy (CSP) Header Not Set)

CWE ID	693
WASC ID	15
Reference	• https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy • https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html • https://www.w3.org/TR/CSP/ • https://w3c.github.io/webappsec-csp/ • https://web.dev/articles/csp • https://caniuse.com/#feat=contentsecuritypolicy • https://content-security-policy.com/

Cross-Domain Misconfiguration

Source raised by a passive scanner (Cross-Domain Misconfiguration)

CWE ID 264

WASC ID 14

Reference
- https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Cookie with SameSite Attribute None

Source raised by a passive scanner (Cookie without SameSite Attribute)

CWE ID 1275

WASC ID 13

Reference
- https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

Strict-Transport-Security Header Not Set

Source raised by a passive scanner (Strict-Transport-Security Header)

CWE ID 319

WASC ID 15

Reference
- https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_SecurityCheat_Sheet.html

https://owasp.org/www- community/Security_Headers

- https://en.wikipedia.org/wiki/ HTTP_Strict_Transport_Security
- https://caniuse.com/ stricttransportsecurity
- https://datatracker.ietf.org/ doc/html/rfc6797

Timestamp Disclosure - Unix

Source (Timestamp Disclosure)	raised by a passive scanner
CWE ID	200
WASC ID	13
Reference	▪ https://cwe.mitre.org/data/definitions/200.html

Information Disclosure - Suspicious Comments **Source**

raised by a passive scanner(Information Disclosure - Suspicious Comments)

CWE ID	**200**
WASC ID	13

Loosely Scoped Cookie

Source	raised by a passive scanner

(Loosely Scoped Cookie)

CWE ID 565

WASC ID 15

Reference
- https://tools.ietf.org/html/rfc6265#section-4.1
- https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html
- https://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies

Re-examine Cache-control Directives **Source** raised by a passive scanner

(Re-examine Cache-control Directives)

CWE ID 525

WASC ID 13

Reference
- https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
- https://grayduck.mn/2021/09/13/cache-control-recommendations/

Retrieved from Cache

Source raised by a passive scanner (Retrieved from Cache)

Reference
- https://tools.ietf.org/html/rfc7234
- https://tools.ietf.org/html/rfc7231
- https://www.rfc-editor.org/rfc/rfc9110.html

Session Management Response Identified

Source raised by a passive scanner (Session Management Response Identified)

Reference
- https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id

User Agent Fuzzer

Source raised by an active scanner (plugin ID: 10104)

Reference
- https://owasp.org/wstg